IEEE Symposium on Security and Privacy 2012 参加報告

松本 晋一† 櫻井 幸一†,‡

†(財)九州先端科学技術研究所
814-0001 福岡市早良区百道浜 2-1-22
smatsumoto@isit.or.jp

‡九州大学大学院システム情報科学研究院情報学部門
819-0395 福岡市西区元岡 744
sakurai@csce.kyushu-u.ac.jp

あらまし 本稿では，2012年5月21日から23日に米国カリフォルニア州サンフランシスコにて開催されたIEEE Symposium on Security and Privacy 2012 [1]，および同月24，25の両日に開催された併催ワークショップ [2] に関し，その概要を報告する.

A Report on IEEE Symposium on Security and Privacy 2012

Shin-ichi Matsumoto† Kouichi Sakurai†, ‡

†Institute of Systems, Information Technologies and Nanotechnologies
2-1-22 Sawara-ku, Fukuoka 814-0001, JAPAN
smatsumoto@isit.or.jp
‡Department of Informatics Faculty of Information Science and Electrical Engineering
744 Motooka Nishi-ku Fukuoka 819-0395, JAPAN
sakurai@csce.kyushu-u.ac.jp

Abstract This paper repots on the 33th IEEE Symposium on Security and Privacy, held on May 21 to 23, 2012 at San Francisco, CA, U.S.A and co-located workshops held on May24 and 25 at the same place.

1 はじめに

本稿[1]では，2012 年 5 月 21 日から 23 日に米国カリフォルニア州サンフランシスコにて開催された IEEE Symposium on Security and Privacy 2012，および同月 24，25 の両日に開催された併催ワークショップに関し，その概要を報告する.

[1]**謝辞** 本研究の一部は，PRACTICE: 国際連携によるサイバー攻撃技術の研究開発(総務省)の支援を受けています.

2 シンポジウム概要

IEEE Symposium on Security and

Privacy (以下，IEEE S&P とする)は，1980 年の初回開催から，今回で 33 回目を数える．初回から昨年度まではカリフォルニア州オークランドで開催されていたが，本会は，サンフランシスコでの開催となった．

主催は IEEE Computer Society on Security and Privacy と IACR(International Association for Cryptologic Reseach)の共催による．スポンサーは以下の各社である．

- Google
- IBM
- CERT, CMU SEI
- Microsoft Research
- NSA
- Symantec
- Lincoln Laboratory, MIT
- Van Pelt, Yi & James LLP(law firm)
- Facebook

本会議の会期は，5 月 21 日(月)から 23 日(水)までの三日間であったが，会期前日の 20 日(日)夕方から受付が開始された．会期初日(21 日)の夜には，ポスターセッション[3]が開催された．また本会議の後，24 日(木)，25 日(金)の両日には，併設の五つのワークショップが開催された．

2.1 運営体制

本大会の運営体制は，以下からなる．

- General chair
  Rob Cunningham (MIT Lincoln Laboratory)
- Program chairs
  Somesh Jha (Univ. of Wisconsin, Madison) and Wenke Lee (Georgia Tech)
- Treasurer
  Greg Shannon (CMU CERT)
- Vice Chair and Registration Chair
  Robin Sommer (ICSI and Lawrence Berkeley National Laboratory)
- Donations Chair
  David Molnar (Microsoft Research)
- Publications Chair
  Kevin Butler (University of Oregon)
- Site Chair
  Ed Talbot (Consultant)
- Publicity and Media Chair
  Ulf Lindqvist (SRI International)
- Student Travel Committee Chair
  Terry Benzel (USC Information Sciences Institute)
- Poster Chair
  Adam Chlipala (MIT)
- Web Chair
  Andrew Johnson (Harvard Univ. and MIT Lincoln Laboratory)

2.2 Call for Paper

IEEE S&P の Call for Paper では，コンピュータセキュリティもしくはプライバシの様々な側面に寄与する研究を募集している．特に関係するトピックとして以下を挙げている．

- アクセス制御
- アカウンタビリティ
- 匿名性
- アプリケーションセキュリティ
- 攻撃と防御
- 認証
- 検閲と検閲対策
- 分散システムセキュリティ
- 組込システムセキュリティ
- フォレンジクス
- ハードウェアセキュリティ
- 侵入検出
- 言語ベースセキュリティ
- マルウェア
- メトリクス
- ネットワークセキュリティ
- プライバシ保護システム
- プロトコルセキュリティ
- セキュア情報フロー
- セキュリティ及びプライバシポリシイ

- セキュリティアーキテクチャ
- システムセキュリティ
- ユーザビリティとセキュリティ
- Web セキュリティ

また 2010 年より，SoK(Systematization of Knowledge) paper と呼ばれる枠が設けられている．これは，これまでに得られた知識を評価し，体系化し，文脈を明らかにする研究を促すことを目的としており，新しい研究的貢献を含まないが，コミュニティに非常に貴重な価値をもたらすものを対象としている．

本年度は SoK 論文として 7 本が採択された．

2.3 投稿論文

表 1 に，本年度を含めた過去 6 回の投稿論文数，採択論文数，採択率を示す．投稿論文数はほぼ毎年漸増しているが，昨年度の投稿数は特に多かった．これに対し本年度は微減している．本年度の採択数は，過去最多であった 2011 年をも上回る 40 本となった．

採択率は例年 11%前後で推移していた．2010 年は採択率が低いが，当該大会では SoK 論文を採択数に含めていない．2011 年と 2012 年は SoK 論文が採択数に含まれており．これを勘案すると 2010 年の採択率はほぼ例年通りとなる．2012 年は，採択数の大幅な増加を受けて若干増加している．

表 1 IEEE S&P の投稿採択論文数

	投稿数	*採択数*	*採択率*
2007 年	246	29	11.8%
2008 年	249	28	11.2%
2009 年	254	26	10.2%
2010 年	267	26	9.7%
2011 年	309	34	11.0%
2012 年	289	40	13.8%

2.4 IEEE S&P 2012 の構成

以下に本年度を含めた過去 3 回のセッション構成を示す．各行の数字は，セッション内の発表論文数を示す．

2012 年

System Security	8
Malware	3
Attacks	6
Foundations	3
Access Control & Attestation	3
Privacy	4
Network Security	3
Web Security	3
Privacy and Anonymity	4
Passwords	3

2011 年

Security of authentication and protection mechanisms	3
Hardware Security	2
Systematization of Knowledge	4
Browsing Security and Privacy	3
Secure Info. Flow and Info. Policies	4
Privacy and Social Networks	3
Virtualization&Trusted Computing	4
Program Security Analysis	3
Underground Economy/Malware	2
Vulnerability Analysis	4
Anonymity and Voting	2

2010 年

Special Papers for the 30th Anniversary of the Symposium	3
Malware Analysis	3
Information Flow	4
Root of Trust	3
Information Abuse	4
Network Security	3
Systematization of Knowledge	5
Secure Systems	3
Analyzing Deployed Systems	3
Language-Based Security	3

セッション構成として，2010 年，2011 年は SoK をまとめて独立したセッションとして設けられていたが，今年は各テーマを掲げるセッション内に組み込まれた形式となった．

2012 年は特に System Security セッションと Attacks セッションの発表件数の多さが目立

つ．前者については，前回では Hadrware Security や Virtualization に分類されていたと思われるテーマが当該セッションに含まれたためと考えられる．また後者については，前回では Vulnerability Analysis や Web Browsing, Anonymity and Voting に分類されていたと思われるテーマが当該セッションに含まれたためと思われる．

一方で Malware の発表については，近年のトピックであるモバイルデバイスのマルウェアについてのものが 3 本中 2 本を占め，また Attack セッションでも Andriod の攻撃手法をテーマにした発表が行われた．更にワークショップでもモバイルデバイスのマルウェアを扱う講演や発表があり，やはり関心の高まりがうかがえた．

3 IEEE S&P における発表

3.1 本会議

発表論文は，40 件であり，その内 SoK 論文が 7 件であった．

S&P 2012 の予稿集は USB メモリに収容されて配布された．また発表時に用いられたスライドのうち，一部の発表のものについては，プログラムの WEB ページから入手可能である．

また Attack 2 セクションの発表 3 件については，発表の模様を動画に収めたものを IEEE S&P の WEB ページ上のリンクから視聴可能である．

Session 1: System Security

[1a]A Framework to Eliminate Backdoors from Response Computable Authentica- tion

[1b]Safe Loading - A Foundation for Secure Execution of Untrusted Programs

[1c]Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints

[1d]ReDeBug: Finding Unpatched Code Clones in Entire OS Distributions

Session 2: Malware

[2a][SoK]Prudent Practices for Designing Malware Experiments: Status Quo and Outlook

[2b]Abusing File Processing in Malware Detectors for Fun and Profit

[2c][SoK]Dissecting Android Malware: Charac- terization and Evolution

Session 3: Attacks 1

[3a]Distance Hijacking Attacks on Distance Bounding Protocols

[3b]Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards

[3c]Memento:Learning Secrets from Process Footprints

Session 4: Foundations

[4a]Foundations of Logic-Based Trust Manage- ment

[4b]Formalizing and Enforcing Purpose Restrictions of Privacy Policies

[4c]Sharing Mobile Code Securely With Infor- mation Flow Control

Session 5: Access Control and Attestation

[5a][SoK]The Psychology of Security for the Home Computer User

[5b]User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems

[5c]New Results for Timing-Based Attestation

Session 6: Privacy

[6a]ObliviAd: Provably Secure and Practical Online Behavioral Advertising

[6b]Quid-Pro-Quo-tocols: Strengthening Semi-Honest Protocols with Dual Execution

[6c]Hummingbird: Privacy at the time of Twitter

[6d]On the Feasibility of Internet-Scale Author Identification

Session 7: Network Security

[7a]Scalable Fault Localization under Dynamic Traffic Patterns

[7b][SoK]Peek-a-Boo, I Still See you: Why Efficient Traffic Analysis Counter-measures Fail

[7c]Off-Path TCP Sequence Number Inference Attack - How Firewall Middleboxes Reduce Security

Session 8: Attacks 2

[8a]Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign- On Web Services

[8b]Unleashing Mayhem on Binary Code

[8c]Clash Attacks on the Verifiability of E-Voting Systems

Session 9: Web Security

[9a][SoK] Third-Party Web Tracking Policy and Technology

[9b]EvilSeed: A Guided Approach to Finding Malicious Web Pages

[9c]Rozzle: De-Cloaking Internet Malware

Session 10: Privacy and Anonymity

[10a]Detecting Hoaxes, Frauds, and Deception in Writing Style Online

[10b]LASTor: A Low-Latency AS-Aware Tor Client

[10c][SoK]OB-PWS: Obfuscation-Based Private Web Search

[10d]LAP: Lightweight Anonymity and Privacy

Session 11: Passwords

[11a]Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms

[11b]The science of guessing: analyzing an anonymized corpus of 70 million passwords

[11c][SoK] The quest to replace passwords: A framework for comparative evaluation of web authentication schemes

Session 12: System Security

[12a]ILR: Where'd My Gadgets Go?

[12b]Space Traveling across VM: Automatically Bridging the Semantic Gap in Virtual Machine Introspection via Online Kernel Data Redirection

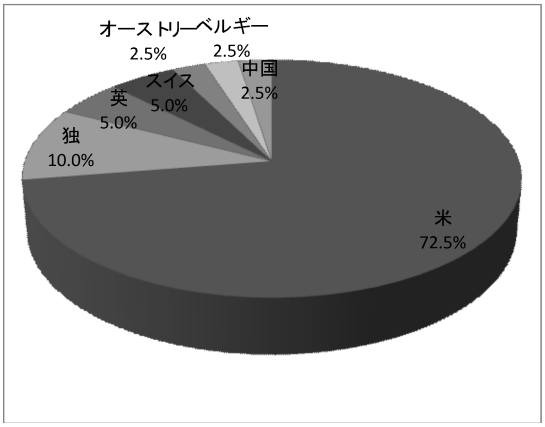
[12c]Smashing the Gadgets: Hindering Return-Oriented Programming Using In-Place Code Randomization

[12d]Building Verifiable Trusted Path on Commodity X86 Computers

発表論文は，グラフ 1 に示す通り，米国からのものが 7 割以上をしめた．アジアからの発表は 1 件のみであった．

また発表は大学からのものが 9 割以上と大多数をしめた．

グラフ 1．発表の国別内訳



3.2 表彰論文

会期二日目に，本会議の発表の表彰が行われた．受賞研究は，以下の 3 件である．

- Best Paper Award

[3b]Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards

- Best Student Award

[3c]Memento: Learning Secrets from Process Footprints

- Best Practical Award

[5b]User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems

3.3　個別発表抜粋

以下に，本会議の発表のうち，特徴的と思われる発表 4 本について要約する.

1) Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards
Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz (Horst-Goertz Institute)

本研究は，衛星携帯電話の標準である GMR-1 および GMR-2 の二方式について，その暗号アルゴリズムの解析と，セキュリティ強度の評価を行っている.

衛星携帯電話の通信方式の詳細は，暗号アルゴリズムも含めて一般に公開されてはいないが，著者らは衛星携帯電話端末のファームウェア更新のために，インターネット上で一般に公開されているイメージファイルを入手し，これを元にリバースエンジニアリングを行うことにより，衛星携帯電話の暗号アルゴリズムを特定している.

著者らは二種類の衛星携帯電話端末について解析を行い，それぞれが採用する二種類の暗号アルゴリズムについて，GMR-1 暗号アルゴリズムが GSM 携帯電話で用いられているストリーム暗号である A5/2 アルゴリズムを改変したものと考えられること，また GMR-2 暗号アルゴリズムは全く新規のストリーム暗号方式と考えられることを明らかにした.

また著者らは更に暗号アルゴリズムの強度解析を行い，GMR-1 については既存の GSM A5/2 アルゴリズムに対する暗号文攻撃を用いて平均 232 ステップで解読が可能なことを示した. また GMR-2 については，選択平文攻撃を用いて，実際的な計算量でセッション鍵を回復可能であることを示した.

本発表は今大会の Best Paper Award を受賞したが，衛星携帯電話という，通信/暗号アルゴリズムの詳細が一般に明らかになっていない方式について，オリジナリティの高い切り口から問題に取り組み，暗号強度解析まで完了させた完成度の高さが評価されたものと思われる.

2) Flash Memory for Ubiquitous Hardware Security Functions: True Random Number Generation and Device Fingerprints
Yinglei Wang, Wing-kei Yu, Shuo Wu, Greg Malysa, G. Edward Suh, and Edwin Kan (Cornell University)

本研究は入手が容易な Flash メモリを用いて真正乱数生成器 (tRNG: true random number generator) 機能と物理複製防止 (PUF: physically unclonable function)を実現する方式を提案している.

Flash メモリへの書き込み(プログラミング)の途中，プログラミングの完了前に中断(abort)させ，完全にプログラミングが完了していない，partial programming と呼ぶ状態を作り出すことで，これらの機能を実現する. プログラミング中の中断は，多くのベンダの製品が備える ONFI (Open NAND Flash Interface)などで可能である.

RNG については，partial programming により，ランダム・テレグラフ・ノイズを作りだすことで実現している. RNG 生成の性能については，NIST の乱数テストをパス可能な乱数を，1 秒あたり最大 10kbit のスループットで生成可能であることを示した.

また PUF については，Flash メモリ製造時の個々のセルの特性のばらつきを利用している. ユニークネス(異なるチップ，ページ間での，フィンガープリント特性の相関係数の小ささ)，ロバストネス(同一ページのフィンガープリント特性の相関係数の大きさ)を検証し，十分な結果を得たとしている.

3) Abusing File Processing in Malware Detectors for Fun and Profit
Suman Jana and Vitaly Shmatikov (University of Texas at Austin)

著者らは，マルウェア検出器におけるマルウェアの走査において，検証対象ファイルの種別の推定を行った後に，その種別に応じたファイルのパース処理を行うという現在のマルウェア検出器の方式に問題があると指摘，二つの攻

撃手法 Chameleon Attack と Warewolf Attack について述べた.

著者は，マルウェア検出器と，OS/アプリケーションとで異なるファイル種別と判定するファイルのパタンの例を明らかにし，このようなファイルによる攻撃を Chameleon Attack と呼んだ.

またマルウェア検出器では解析できないが，OS やアプリケーションでは解析可能なファイルのパタン例を明らかにし，このようなファイルを用いた攻撃を Warewolf Attack と呼んだ.

著者らは，これら二種類の攻撃への対策として，マルウェア検出器におけるファイル種別判定のアルゴリズムとファイル内容の解析処理のアルゴリズムを，OS/アプリケーションと同じものにする必要性について述べている.

4) Memento:Learning Secrets from Process Footprints
Suman Jana and Vitaly Shmatikov (University of Texas at Austin)

本研究は，単一端末をマルチユーザで共有する環境において，別ユーザの行動を追跡するサイドチャネル攻撃を扱っている.

例えば UNIX OS においては，OS 上で動作中のプロセス全ての DRS(Data Resident Size)を，/proc/<pid>/statm 内の drs フィールドから確認できる. これにより他ユーザの DRS も確認できる.

著者らはこの DRS の時系列変化を取得し，予め作成したシグネチャと照合することで，他ユーザが閲覧中の WEB ページを 30~50%の確度で識別可能であることを示した. 確度は WEB ブラウザの種類によって異なる.

近年，UNIX ワークステーションを複数ユーザで共用する運用は稀となりつつあるが，Android OS ではユーザ ID をアプリケーションの識別に用いていることから，本攻撃手法を用いることで，同一携帯端末上の他アプリケーションの動作を知ることができるという，プライバシ上の問題をはらんでいると指摘している.

本発表は今大会の Best Student Award に選ばれた. マルチユーザ環境のサイドチャネル攻撃が，現在注目を集めている Android マルウェアに転じる可能性についてという着眼点のユニークさが評価されたものと思われる.

3.4 ポスターセッション

ポスターセッションは会期初日である 21 日の夜に，レセプションの場で行われ，以下のカテゴリに沿って，37 本の展示が行われた.

- Security & Privacy for Shared Databases
- Internet
- Detecting, Analyzing & Preventing Attacks
- Software Interfaces & Correctness
- Wireless, Mobile, & Embedded
- Potpourri
- Workshops

3.5 ワークショップ

IEEE S&P では会期後の二日間で以下のワークショップが開催された. 各ワークショップは一日間の会期であり，このうち W2SP と MoST, WSCS は 24 日に平行して開催され，WRIT と TrustED は 25 日に平行して開催された. ワークショップの予稿集は CD-ROM で配布されたが，一部の発表については，各ワークショップの WEB ページから参照できる.

・ W2SP: Web 2.0 Security and Privacy [4]

Web 2.0 におけるセキュリティとプライバシの問題にフォーカスしたワークショップであり，2007 年より IEEE S&P 本会議との併催が続いており，本年で 5 回目の開催である.

1 件の基調講演と，11 件の研究発表(うち 4 件は MoST とのジョイントセッション内での発表)が行われた.

殆どの発表については，予稿が WEB サイトから参照可能である.

・ MoST: Mobile Security Technologies [5]

モバイルデバイスやアプリケーション，システムの研究者や開発者などを対象として，モバイルデバイスハードウェアや OS,ミドルウェアなどのセキュリティについて扱うワークショップであ

り，基調講演 1 件と 14 件の研究発表(うち 4 本は W2SP とのジョイントセッションでの発表)が行われた.

一部の発表については，予稿やスライドが WEB サイトから参照可能である.

・ WRIT: Workshop on Research for Insider Threat [6]

特にインサイダーからのセキュリティ上の脅威(IT: Insider Threat)にフォーカスしたワークショップであり，IT 問題の固有の側面についてと，IT 防御，検出と緩和のための技術的アプローチについて，また IT に関する経験と評価，データセットについて論じる.

8 件の研究発表とパネルディスカッションが行われた.

・ WSCS: Workshop on Semantic Computing and Security [7]

コンテンツからセマンティクスを抽出し利用を図るセマンティックコンピューティング技術と，コンピュータネットワーク上でのセキュアな振る舞いとセキュアでない振る舞いを識別するセキュリティ技術を組み合わせ，活用を図るワークショップであり，1 件の基調講演と 12 件の研究発表が行われた.

・ TrustED: Workshop on Special Aspects of Cyber Physical Systems: Trustworthy Embedded Systems [8]

サイバーフィジカルシステムとその環境にフォーカスしたワークショップであり，今回で 2 回目を数える(前回開催は ESORICS 2011 との併催). 3 件の招待講演と，5 件の研究発表が行われた.

研究発表については，発表に用いられたスライドが WEB ページから参照できる.

4 IEEE S&P 2013 について

IEEE S&P 2012 会期最終日に，次回開催の概要(開催場所と会期)が発表されたが，その後変更された模様である. 変更を伝える WEB ページによると，IEEE S&P 2013 の会期は 2013 年 5 月 14 日から 24 日，場所はカリフォルニア州バークレイとアナウンスされている. 現時点では Call for Paper に関する詳細は公開されていない.

5 おわりに

本稿では，2012 年 5 月 21 日から 25 日に米国カリフォルニア州サンフランシスコにて開催された IEEE S&P 2012，および同月 24，25 両日に開催された併催ワークショップに関し，その概要を報告した.

参考文献

[1]IEEE Symposium on Security and Privacy 2012
http://www.ieee-security.org/TC/SP2012/index.html

[2]IEEE Symposium on Security and Privacy 2012 Workshops
http://ieee-security.org/TC/SPW2012/

[3]Poster Session
http://www.ieee-security.org/TC/SP2012/posters.html

[4]W2SP 2012: Web 2.0 Security & Privacy 2012
http://www.w2spconf.com/2012/

[5]MoST 2012: Mobile Security Technologies 2012
http://mostconf.org/2012/

[6]Workshop on Research for Insider Threat(WRIT)
http://ieee-security.org/TC/SPW2012/writ-website/writ.php

[7]Workshop on Semantic and Security (WSCS)
http://ieee-security.org/TC/SPW2012/wscs-website/wscs.php

[8]TrustED | Trustworthy Embedded Devices
http://trusted.trust.cased.de/